THE NEW CMMC & OTHER SECURITY REQUIREMENTS FROM 3 PERSPECTIVES:
DOD, SUPPLY CHAIN, AND LEGAL

Presented by:

Bhavesh Vadhani, Partner, CohnReznick LLP
Rebecca Kehoe, Manager, CohnReznick LLP
Mark Maier, Partner, Shulman Rogers

Dec 10 and 18, 2019
PLEASE READ

This presentation has been prepared for information purposes and general guidance only and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice.

No representation or warranty (express or implied) is made as to the accuracy or completeness of the information contained in this publication, and CohnReznick LLP, its members, employees and agents accept no liability, and disclaim all responsibility, for the consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

This presentation and its content are the property of CohnReznick LLP and are protected by applicable copyright laws. Any unauthorized use of the information herein will be considered a violation of CohnReznick LLP’s intellectual property rights. Unless stated otherwise herein, no part of this presentation may be copied, distributed, or published, in whole or in part, without the prior written agreement of CohnReznick LLP.
AGENDA

• Cybersecurity Maturity Model Certification (CMMC)
• Supply Chain Risk Management (SCRM)
• Prime contractor’s responsibility and flow downs to sub-contractors
• Suspension and debarment resulting from failure to comply with requirements
• Liabilities for false claims about cyber security
Source: GAO High Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation

September 2018
CMMC OVERVIEW

• Cybersecurity Maturity Model Certification (CMMC) will be a new standard and maturity model used by DoD in assessing government contractors cybersecurity maturity

• CMMC framework to be released in Jan 2020 with certification to be ready for issuance in Fall 2020
  • Best practices categorized in Domains
  • Domains further segmented by a set of capabilities
  • Capabilities demonstrated by adherence to practices and processes

• The required CMMC level (notionally between 1 - 5) for a specific contract will be contained in the RFP sections L & M, and will be a “go/no-go decision”

Source: CMMC v0.6b-20191107
CMMC will have five different levels of maturity ranging from basic hygiene to advanced/progressive.

**Level 1**
- Technical Practices: Demonstrate basic cyber hygiene, as achieved by the Federal Acquisition Regulation (FAR)
- Process Maturity: No process maturity

**Level 2**
- Technical Practices: Demonstrate intermediate cyber hygiene
- Process Maturity: Standard operating procedures, policies, and plans are established for all practices

**Level 3**
- Technical Practices: Demonstrate good cyber hygiene and effective NIST SP 800-171 Rev 1 security requirements
- Process Maturity: Activities are reviewed for adherence to policy and procedures and adequately resourced

**Level 4**
- Technical Practices: Demonstrate a substantial and proactive cybersecurity program
- Process Maturity: Activities are reviewed for effectiveness and management is informed of any issues

**Level 5**
- Technical Practices: Demonstrate a proven ability to optimize capabilities in an effort to repel advanced persistent threats
- Process Maturity: Activities are standardized across all applicable organizational units and identified improvements are shared
CMMC MODEL DOMAINS

17 Control Families

Domains:
- 48 FAR 52.204-21
- NIST 800-171r1
- Draft NIST SP 800-171B

Practices:
- CMMC
- NIST 800-171/NIST CSF
- UK NCSC Cyber Essentials
- ISO/IEC 27001
- CERT RMM
- AU ACSC Essential Eight
- CIS Controls

Source: CMMC v0.6b-20191107
## CMMC Domain and Capabilities

List of capabilities for each domain

<table>
<thead>
<tr>
<th>Domain</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Establish system access requirements</td>
</tr>
<tr>
<td></td>
<td>Control internal system access</td>
</tr>
<tr>
<td></td>
<td>Control remote system access</td>
</tr>
<tr>
<td></td>
<td>Limit data access to authorized users and processes</td>
</tr>
<tr>
<td>Asset Management</td>
<td>Identify and document assets</td>
</tr>
<tr>
<td>Audit and Accountability</td>
<td>Define audit requirements</td>
</tr>
<tr>
<td></td>
<td>Perform auditing</td>
</tr>
<tr>
<td></td>
<td>Identify and protect audit information</td>
</tr>
<tr>
<td></td>
<td>Review and manage audit logs</td>
</tr>
<tr>
<td>Awareness and Training</td>
<td>Conduct security awareness activities</td>
</tr>
<tr>
<td></td>
<td>Conduct training</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Establish configuration baselines</td>
</tr>
<tr>
<td></td>
<td>Perform configuration and change management</td>
</tr>
<tr>
<td>Identification and Authentication</td>
<td>Grant access to authenticated entities</td>
</tr>
<tr>
<td>Incident Response</td>
<td>Plan incident response</td>
</tr>
<tr>
<td></td>
<td>Detect and report events</td>
</tr>
<tr>
<td></td>
<td>Develop and implement a response to a declared incident</td>
</tr>
<tr>
<td></td>
<td>Perform post incident reviews</td>
</tr>
<tr>
<td></td>
<td>Test incident response</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance</td>
<td>Manage maintenance</td>
</tr>
<tr>
<td>Media Protection</td>
<td>Identify and mark media</td>
</tr>
<tr>
<td></td>
<td>Protect and control media</td>
</tr>
<tr>
<td></td>
<td>Sanitize media</td>
</tr>
<tr>
<td></td>
<td>Protect media during transport</td>
</tr>
<tr>
<td>Personnel Security</td>
<td>Screen personnel</td>
</tr>
<tr>
<td></td>
<td>Protect federal contract information during personnel actions</td>
</tr>
<tr>
<td>Physical Protection</td>
<td>Limit physical access</td>
</tr>
<tr>
<td>Recovery</td>
<td>Manage back-ups</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Identify and evaluate risk</td>
</tr>
<tr>
<td></td>
<td>Manage risk</td>
</tr>
<tr>
<td>Security Assessment</td>
<td>Develop and manage a system security plan</td>
</tr>
<tr>
<td></td>
<td>Define and manage controls</td>
</tr>
<tr>
<td></td>
<td>Perform code reviews</td>
</tr>
<tr>
<td>Situational Awareness</td>
<td>Implement threat monitoring</td>
</tr>
<tr>
<td>Systems and Communications</td>
<td>Define security requirements for systems and communications</td>
</tr>
<tr>
<td>Protection</td>
<td>Control communications at system boundaries</td>
</tr>
<tr>
<td>System and Information Integrity</td>
<td>Identify and manage information system flaws</td>
</tr>
<tr>
<td></td>
<td>Identify malicious content</td>
</tr>
<tr>
<td></td>
<td>Perform network and system monitoring</td>
</tr>
<tr>
<td></td>
<td>Implement advanced email protections</td>
</tr>
</tbody>
</table>

Source: CMMC v0.6b-20191107
# CMMC PROCESS MATURITY

Process for each maturity level (ML)

<table>
<thead>
<tr>
<th>Process Maturity Level</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ML 1: Performed</td>
<td><em>There are no maturity processes assessed at ML 1. A Level 1 organization performs Level 1 practices but does not exhibit process institutionalization.</em></td>
</tr>
</tbody>
</table>
| ML 2: Documented       | 1. Establish a policy that includes [DOMAIN NAME]  
                        | 2. Establish practices to implement the [DOMAIN NAME] policy  
                        | 3. Establish a plan that includes [DOMAIN NAME] |
| ML 3: Managed          | 1. Review [DOMAIN NAME] activities for adherence to policy and practices  
                        | 2. Provide adequate resources for [DOMAIN NAME] activities |
| ML 4: Reviewed         | 1. Review and measure [DOMAIN NAME] activities for effectiveness  
                        | 2. Inform high-level management of any issues with [DOMAIN NAME] activities |
| ML 5: Optimized        | 1. Standardize a documented approach for [DOMAIN NAME] across all applicable organizational units  
                        | 2. Share identified improvements to [DOMAIN NAME] activities across the organization |

Source: CMMC v0.6b-20191107
“We need risk management solutions to assess, measures, and mitigate risk in real-time across multi-tier partner and supplier networks to achieve our goal of cost, schedule and performance, as they are only effective in a secure environment.”

- The Honorable Kevin Fahey, Assistant Secretary of Defense for Acquisition

Source: Securing the Supply Chain Presentation – Katie Arrington
POLLING QUESTION

- Has your organization implemented security controls using NIST 800-171/171B or NIST 800-53 that can potentially help satisfy CMMC requirements?
  - Yes
  - No
  - Not sure
SUPPLY CHAIN RISK MANAGEMENT (SCRM)

Supply Chain Risk

The potential exposure to problems, harm or loss that arise from relying on outside parties to perform services or activities on your behalf.

Supply Chain Risk Management (SCRM)

Supply Chain Risk Management (SCRM) is the process of analyzing and controlling risks presented to your company, your data, your operations and your finances by parties involved in your supply chain.

How Did We Get Here?

- Growing sophistication of Information and Communication Technology (ICT)
- Number and scale of information systems
- Increasing reliance on COTS
- Speed and scale of globalization
- Complex supply chain (logically long and geographically diverse)
- Significant increase in the number of entities who ‘touch’ products and services
- Natural disasters, poor product/service quality and poor security practices
- Lack of visibility and understanding: how technology is developed, integrated and deployed and practices to assure security.
- Lack of transparency on financial status, business and labor practices
- A lack of control of the decisions impacting the inherited risks and ability to effectively mitigate those risks.
**FOUR PILLARS OF SCRM**

**Security** provides the confidentiality, integrity, and availability of information that:
- Describes the ICT supply chain (e.g., information about the paths of ICT products and services, both logical and physical); or
- Traverses the ICT supply chain (e.g., intellectual property contained in ICT products and services), as well as information about the parties participating in the ICT supply chain (anyone who touches an ICT product or service throughout its life cycle).

**Integrity** is focused on ensuring that the ICT products or services in the ICT supply chain are genuine, unaltered, and that the ICT products and services will perform according to acquirer specifications and without additional unwanted functionality.

**Resilience** is focused on ensuring that ICT supply chain will provide required ICT products and services under stress or failure.

**Quality** is focused on reducing vulnerabilities that may limit the intended function of a component, lead to component failure, or provide opportunities for exploitation.
TYPES OF SUPPLY CHAIN RISKS

Reputational
Risk of your organization receiving negative public opinion due to problems with, or failure of, a supplier or service provider.

Strategic
Risk arising from your inability to implement strategies or strategic initiatives due to supplier advice/failure.

Operational
Risk of disruption to operations due to the failure in a vendor’s processes, people or systems.

Transactional
Risk of financial loss or damage to credit due to your inability to deliver important services, or transact business, due to problems created by a supplier or even fraud.

Compliance
Risk related to your violation of laws, policies, or regulations due to something the supplier does (or doesn’t do).

Data Information Security
Risk related to the exposure of non-public information (yours and your members, customers, clients’) information due to breach or other fault of a supplier.
SCRM – NIST 800-161

- Provides guidance to federal agencies and its contractors on selecting and implementing mitigating processes and controls at all levels in their organizations to help manage risks to or through ICT supply chains for systems categorized as HIGH according to Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems


- Refines and expands NIST SP 800-53 Rev4 controls, adds new controls that specifically address ICT SCRM, and offers SCRM-specific supplemental guidance where appropriate
THE ICT SUPPLY CHAIN DEFINED

NIST SP 800-161 defines the Information and Communications Technology (ICT) supply chain as follows:

“Any public and private sector entities (e.g., acquirers, system integrators, suppliers, and external service providers) and technology, law, policy, procedures, and practices that interact to design, manufacture, distribute, deploy, and use ICT products and services.”

Provide goods and services for your own or clients’ use

Perform outsourced functions on your behalf

Provide access to markets, products and other types of services
POLLING QUESTION

• Does your organization have a Supply Chain Risk or a Vendor Risk Management Program?
  – Yes
  – No
  – Not Sure
RECENT SCRM TRENDS AND STATS

Source: Aravo, Key Findings from Global Third Party Risk Benchmarking Survey, 2018
PRIME CONTRACTOR RESPONSIBILITIES OVER SUBCONTRACTOR
When DFARS 252.204-7008 and/or 252.204-7012 is applicable, contractors must implement the security requirements specified in the National Institute of Standards and Technology (NIST) Special Publication (SP), Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. The Contractor's purchasing system will be evaluated to assess that:

(a) The contractor's covered defense information flowdown procedures ensure that DoD marking and dissemination statements, contractual requirements on contract deliverables, and DoD government furnished information, that contains marking and dissemination requirements, flow down appropriately to their subcontractors.

(b) The contractor's procedures assure subcontractor compliance with DFARS Clause 252.204-7012.
Policy and Procedures Review:

When reviewing the contractor’s supply chain management policies and procedures the CPSR Analyst should ensure that the contractor’s policy, at a minimum, requires the flow down of DFARS 252.204-7012, when applicable, including the content of paragraph (m), Subcontracts, which states that the contractor shall:

(a) include this clause, in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties. The Contractor shall determine when the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer/requiring activity; and
(b) Require subcontractors to:

i. Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

ii. Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber-incident to DoD as required in paragraph (c) of DFARS 252.204-7012.
File Reviews:

- DCMA will review subcontracts/POs to determine if the contractor has flowed down DFARS 252.204-7012 in all applicable procurement files within the selected sample.

- DCMA will validate that covered defense information is properly marked in procurement files containing DFARS 252.204-7012.

- Prime’s need to be aware that no covered defense information should be present in procurement files where DFARS 252.204-7012 is not included.
The contractor will be asked by DCMA to show how they have determined that the subcontractor has a covered contractor information system that can receive and protect covered defense information, to include an adequate System Security Plan.

However this requires the Prime Contractor to have personnel who are experts in the NIST SP 800-171 requirements such that they can assess whether a System Security Plan meets those requirements.

And the DCMA Guidebook is silent on whether actual testing by the Prime Contractor of the Subcontractor’s IT systems would be required.
DCMA CPSR GUIDEBOOK

• An alternate acceptable method would be for the subcontractor to present the contractor with a basic self-assessment of compliance with the NIST SP 800-171 security requirements.
  • However, the Prime Contractor cannot just blindly accept “self-assessments” from subcontractors, especially if the subcontractor is small or mid size and does not, in general, have sophisticated IT systems and personnel.
  • DCMA is silent on whether a 3rd Party assessment would be acceptable, a reputable 3rd party assessment would be better than a self assessment.
POLLING QUESTION

• Does your organization conduct or require third party audits of your sub contractors IT environment as it relates to security?
  – Yes
  – No
  – Not Sure
LEGAL LIABILITIES AND MITIGATIONS
No Attorney-Client Relationship
Not Legal Advice
SUSPENSION AND DEBARMENT

• Immediate Suspension
  – Violations: Adequate evidence of a crime of Fraud, Antitrust, Theft, Tax...
    • Including false statements on cybersecurity such as DFARS and CMMC
  – Period: <1 year

• Debarment
  – Violations:
    • Civil conviction for Fraud, Antitrust, Theft, Integrity, ...
    • Preponderance for willful or repeating contract Breach, Tax, ...
  – Period: General <3 years, Drugs <5, Arms control >2, ... +extended

• Penalties
  – Personal: Imputed to individuals who knew or had reason to know
FALSE CLAIMS

• Violations
  – Knowing, reckless disregard, deliberate ignorance
  – Conspires to or makes
  – False Claim for payment, material statement, certification without completely knowing the information, …
    • Cybersecurity requirements like DFARS 7012 & CMMC can be material

• Penalties
  – $11-22K for each false claim
  – Plus triple government’s damages

• Qui Tams relator receives 15-25% of the recovery
GOV CON DEFENSE AND SAFETY ACT

• Government Contractor Defense
  – Immunity from state and federal tort liability
    • US approved reasonably precise specifications
    • Equipment conformed to those specifications
    • OEM warned the US about dangers

• SAFETY Act
  – Products and services, including cybersecurity
  – Identify, detect, deter, respond to or mitigate terrorism
  – Designation
    • Liability capped at insurance
    • Exclusive Federal Court
    • Recovery reduced by other sources, no punitives, etc
  – Certification: Plus Government Contractor Defense
QUESTIONS & ANSWERS
CONTACT US

Bhavesh Vadhani, CISA, CRISC, CGEIT
Principal
Technology Risk, Cybersecurity, and Privacy
Tysons, VA

703-847-4418
Bhavesh.Vadhani@cohnreznick.com

Rebecca Kehoe, JD
Manager
Government Contracting Industry Practice
Tysons, VA

703-847-4431
Rebecca.Kehoe@cohnreznick.com

Mark Maier, Esq, MCSE, CIPP
Partner & Chair, Government Contracting and Technology Transactions
UA Army Colonel (Retired) & Electrical Engineer
Potomac, MD

301-231-0945
MMaier@ShulmanRogers.com
NEXT LUNCH & LEARN
M&A FOR GOVT. CONTRACTORS: A ROADMAP FOR SUCCESS

Join us for a complimentary Lunch & Learn session on January 13 in Tysons, VA and January 14 Columbia, MD

Mergers and acquisition in the government contracting community are on the rise with multiples higher than ever. However, is your company ready for the due diligence and requirements that come with it? Join CohnReznick, McLean Group, and Protorae Law as they share their sell side and buy side transactional expertise and discuss how transactions affect government contractors’ day to day business, how to develop a plan to prepare and makes it as successful process, and strategies for completing the implementation without breaking the bank while managing risks.

Panelists:

Christine Williamson, CPA, Partner, CohnReznick (moderator)

Jeffrey Michelson, CPA, Managing Director, CohnReznick

David Kuhnsman, Member, Protorae Law

Greg Woodford, Senior Managing Director, The McLean Group